IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

ANN JONES, individually and on behalf of all others similarly situated, Plaintiff, v. BLOOMINGDALE'S.COM, LLC, Defendant.	Case No. 4:22-cv-01095-SEP **JURY TRIAL DEMANDED**

FIRST AMENDED COMPLAINT - CLASS ACTION

Plaintiff Ann Jones ("Plaintiff"), individually and on behalf of all others similarly situated, hereby files this class action complaint against Bloomingdales.com, LLC ("Defendant" or "Bloomingdale's"), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against Bloomingdale's for surreptitiously intercepting and wiretapping the electronic communications of visitors to its website, www.bloomingdales.com. Bloomingdale's procures third-party vendors, such as FullStory, to utilize "session replay" spyware to intercept Plaintiff's and the Class members' electronic computer-to-computer data communications ("Electronic Communications") with Bloomingdale's website, which then deploys on each website visitor's internet browser for the purpose of intercepting and recording the website visitor's electronic communications with the Bloomingdale's website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), search terms, URLs of web pages visited, as well as everything Plaintiff and the Class Members did on those pages, *e.g.*, what they searched for, what

they looked at, the information they inputted, and what they clicked on, and/or other electronic communications in real-time ("Website Communications").

2. The "session replay" spyware utilized by Defendant is not a traditional website cookie, tag, web beacon, or analytics tool. It is a sophisticated computer spyware that allows Defendant to contemporaneously intercept, capture, read, observe, re-route, forward, redirect, and receive incoming Electronic Communications to its website. Plaintiff's and Class Members' Electronic Communications are then stored by Defendant using an outside vendor's services and can later be viewed and utilized by Defendant to create a session replay, which is essentially a video of a Class Member's entire visit to Defendant's website. It results in the electronic equivalent of "looking over the shoulder" of each visitor to the Bloomingdale's website for the entire duration of their website interaction.

3. Bloomingdale's conduct violates the Missouri Wiretap Act, Mo. Ann. Stat. §§ 542.400 *et seq.*, the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010 *et seq*., the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1) *et seq.*, 18 U.S.C. § 2511(3)(a) *et seq*., and 18 U.S.C. § 2701 *et seq*; Title II, 18 U.S.C. § 2702 *et seq*; the Computer Fraud and Abuse Act, ("CFAA") 18 U.S.C. § 1030, *et seq*.; and constitutes an invasion of the privacy rights of website visitors; a trespass to chattels; and conversion to chattels.

4. Plaintiff brings this action individually and on behalf of all natural persons in the United States whose Electronic Communications were intercepted through Defendant's procurement and use of session replay technology embedded in www.bloomingdales.com. (the "Nationwide Class") and on behalf of a sub-class of all natural persons in the State of Missouri whose Electronic Communications were intercepted through Defendant's procurement and use of session replay technology embedded in www.bloomingdales.com (the "Missouri Class") and seeks

all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys' fees and costs.

PARTIES

5. Plaintiff Ann Jones is a citizen of the State of Missouri, and at all times relevant to this action, resided and was domiciled in St. Louis County, Missouri. Plaintiff is a citizen of Missouri.

6. Defendant Bloomingdales.com, LLC is a corporation organized under the laws of Ohio, and its principal place of business is located at 3 Jackson Tower, 20th Floor, 28-07 Jackson Avenue, Long Island City, NY 11101. Defendant is deemed a citizen of Ohio and New York. Defendant can be served through its registered agent Corporate Creations Network Inc. located at 600 Mamaroneck Avenue, Suite 400, Harrison, NY, 10528.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including Plaintiff, is a citizen of a state different than Defendant.

8. This Court further has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this action arises under 18 U.S.C. § 2510, *et seq.*, 18 U.S.C. § 2701, *et seq.*, and 18 U.S.C. § 1030, *et seq.*, and this Court has supplemental jurisdiction over the remaining state law claims pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

9. This Court has personal jurisdiction over Defendant because a substantial part of

the events and conduct giving rise to Plaintiff's claims occurred in Missouri. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Missouri while they were located within Missouri. Defendant markets its products online via its website and ships products to Missouri residents—*i.e.*, Defendant intends for Missouri residents to purchase its products online and, in turn, delivers its products to Missouri. During this process, Plaintiff alleges Defendant surreptitiously intercepted and wiretapped Plaintiff's Electronic Communications on its website while Plaintiff and Class Members were located in Missouri. At all relevant times, Defendant knew that its practices would directly result in collection of information from Missouri citizens while those citizens browse www.bloomingdales.com. Defendant chose to avail itself of the business opportunities of marketing and selling its goods in Missouri and collecting real-time data from website visit sessions initiated by Missourians while located in Missouri, and the claims alleged herein arise from those activities.

10. Bloomingdale's also knows that many users visit and interact with Bloomingdale's websites while they are physically present in Missouri. Both desktop and mobile versions of Bloomingdale's website allow a user to search for nearby stores by providing the user's location, as does the Bloomingdale's app. Users' employment of location services in this way means that Bloomingdale's is continuously made aware that its website is being visited by people located in Missouri, and that such website visitors are being wiretapped in violation Missouri statutory and common law. In fact, Bloomingdale's and Bloomingdales.com's Notice of Privacy Practices on the date on which the case was filed (as archived by the Internet Archive Wayback Machine[1])

[1] https://web.archive.org/web/20221012212234/https://customerservice-bloomingdales.com/articles/bloomingdales-and-bloomingdalescom-notice-of-privacy-practices#Ownership-of-Customer-Data

provided the following:

> Ownership of Customer Data
> […] A change in data ownership may or may not include a notice on the primary online sites of Bloomingdale's or affected subsidiary sites.

11. The customer data that Bloomingdale's purports to own – in violation of Plaintiff's and the Class's rights – is located in Missouri (as to Plaintiff and other Missourians) – making Bloomingdale's subject to personal jurisdiction in Missouri.

12. Moreover, Bloomingdale's is a subsidiary of Macy's, Inc. ("Macy's). "Macy's operates department stores under the nameplates Macy's and Bloomingdale's, and specialty stores that include Bloomingdale's The Outlet, Bluemercury and Macy's Backstage."[2] There are approximately 11 Macy's stores[3] in Missouri thus also giving rise to personal jurisdiction over Bloomingdale's. Additionally, a Market by Macy's recently opened in Saint Louis County, Missouri – within this specific District. Additionally, Bloomingdale's places session replay technology on computers and/or mobile devices whose situs is Missouri – and in computers and mobile devices around the country. Additionally, upon information and belief, Bloomingdale's is represented by the same law department as Macy's. *See*, e.g., https://customerservice-bloomingdales.com/articles/bloomingdales-terms-of-use (Notices and counter-notices should be sent to: Copyright Agent, c/o Macy's Law Department, 13th Floor, 151 West 34th Street, New York, NY 10001 or to Infringement.Response@macys.com.)

13. In addition to the reasons stated above, the Court should find Bloomingdale's, as a subsidiary of Macy's, has sufficient contacts with Missouri. As such, it would not offend the "traditional notion of fair play and substantial justice" to order Bloomingdale's to defend the

[2] https://www.macysinc.com/about/store-count-and-square-footage (last visited: January 18, 2023).
[3] https://www.mallscenters.com/brands/macy-s/missouri (last visited: January 18, 2023).

claims lodged against it in Missouri.

14. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

15. The "world's most valuable resource is no longer oil, but data."[4]

16. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data (*i.e.*, customers' purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.[5] This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.[6]

17. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by

[4] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data.
[5] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, Business News Daily (Aug. 5, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.
[6] *Id.*

85 percent in sales growth and more than 25 percent in gross margin."[7]

18. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[8] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[9]

19. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military record is estimated to cost USD 55."[10]

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

20. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that "a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[11]

21. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party

---

[7] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

[8] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

[9] *Id.* at 25.

[10] *Id.*

[11] Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/.

they know nothing about.[12] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[13]

22. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

23. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[14]

24. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[15]

25. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not

[12] *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html.

[13] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

[14] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[15] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/.

to allow such tracking.[16]

C. How Session Replay Technology Works.

26. Session replay technology, such as that implemented on www.bloomingdales.com, enables website operators to record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by recording website visitors "as they click, scroll, type or navigate across different web pages."[17]

27. While session replay technology is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, session replay technology allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, or has not finished submitting the data to the website operator.[18] As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."[19]

28. Session replay technology works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the

---

[16] Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[17] Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/.

[18] *Id.*

[19] Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0.

occurrence of actions the user takes. When a website delivers session replay technology to a user's browser, the browser will follow the code's instructions by sending responses in the form of "event" data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the session replay technology, rather than the owner of the website where the code is installed.

29. The types of events captured by session replay technology vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through the website. In order to permit a reconstruction of a user's visit accurately, the session replay technology must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

30. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the third party vendor.

31. Once the events from a user session have been recorded by the session replay technology, a website operator can view a visual reenactment of the user's visit through the third party vendor, usually in the form of a video, meaning "[u]nlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions."[20]

32. Because most session replay technology will by default indiscriminately capture

[20] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.[21]

33. Most alarming, session replay technology may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the third party vendor. For example, if a user writes information into a text form field, but then chooses not to click a "submit" or "enter" button on the website, the session replay technology may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the third party vendor.

34. Session replay technology does not necessarily anonymize user sessions, either.

35. First, if a user's entry of personally identifying information is captured in an event response, that data will become known and visible to both the third party vendor and the website owner.

36. Second, if a website displays user account information to a logged-in user, that content may be captured by session replay technology.

37. Third, some third party vendors explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.[22]

---

[21] *Id.*

[22] *Id.*; *see also FS.identify – Identifying users*, FullStory, https://help.fullstory.com/hc/en-us/articles/360020828113, (last visited Sep. 8, 2022).

38. Third party vendors often create "fingerprints" that are unique to a particular user's combination of device and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the third party vendor monitors.

39. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the third party vendor can then associate the fingerprint with the user identity and can then back-reference all of that user's other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

40. In addition to the privacy invasions caused by the diversion of user communications with websites to third party vendors, session replay technology also exposes website visitors to identity theft, online scams, and other privacy threats.[23] Indeed, "[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected [ ] it may not be stored properly or have standard protections" increasing "the overall risk that data will someday publicly leak or be breached."[24]

41. Recognizing the privacy concerns posed by session replay technology, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal

[23] Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720.

[24] Lily Hay Newman, *Covert 'Replay Sessions' Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/.

from the app store.[25] In announcing this decision, Apple stated: "Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity."[26]

D. Bloomingdale's Secretly Wiretaps its Website Visitors' Electronic Communications.

42. Bloomingdale's operates the website www.bloomingdales.com. Bloomingdale's is an online and brick-and-mortar fashion retailer, offering men's and women's apparel, accessories, shoes, and more.

43. However, unbeknownst to the millions of individuals perusing Bloomingdale's products online, Bloomingdale's intentionally procures and embeds various session replay technology from a third party vendor on its website to track and analyze website user interactions with www.bloomingdales.com. Because the third party vendors are unknown eavesdroppers to visitors to www.bloomingdales.com, they are not parties to website visitors' Website Communications with Bloomingdale's.

44. One such third party vendor that Bloomingdale's engages is FullStory.

45. FullStory is the owner and operator of a session replay technology titled FullStory Script, which records all website visitor actions, including information typed by the website users while on the website. Such information can include names, emails, phone numbers, addresses, social security numbers, dates of birth, and more; research by the Princeton University Center for Information Technology Policy found that "text typed into forms is collected before the user

[25] Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), https://techcrunch.com/2019/02/07/apple-glassbox-apps/.
[26] *Id.*

submits the form, and precise mouse movements are saved, all without any visual indication to the user."[27]

46. As a user interacts with any website with the embedded FullStory Script, "each click, tap, URL visit, and every other interaction is sent in tiny little packets to that existing session at FullStory servers."[28] This includes button clicks, mouse movements, scrolling, resizing, touches (for mobile browsers), key presses, page navigation, changes to visual elements in the browsers, network requests, and more.[29]

47. Bloomingdale's knowingly derives a benefit and/or information from the Website Communications intercepted and recorded at its direction. Upon information and belief, Bloomingdale's uses the intercepted Website Communications to replay website visitors' interactions with www.bloomingdales.com, improve user interactions with its website, and to provide targeted advertisements to its website visitors.

48. Bloomingdale's procurement and use of FullStory's session replay technology, and procurement and use of other session replay technology through various third party vendors, and its knowing derivation of a benefit and/or information from the Website Communications surreptitiously intercepted and recorded by session replay technology is a violation of Missouri statutory and common law.

E. Plaintiff's and Class Members' Experience.

---

[27] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

[28] *Id.*

[29] *How does FullStory capture data to recreate my users' experience?*, FullStory, https://help.fullstory.com/hc/en-us/articles/360032975773-How-does-FullStory-capture-data-to-recreate-my-users-experience-, (last visited Aug. 18, 2022) (hereinafter "FullStory Data Capture").

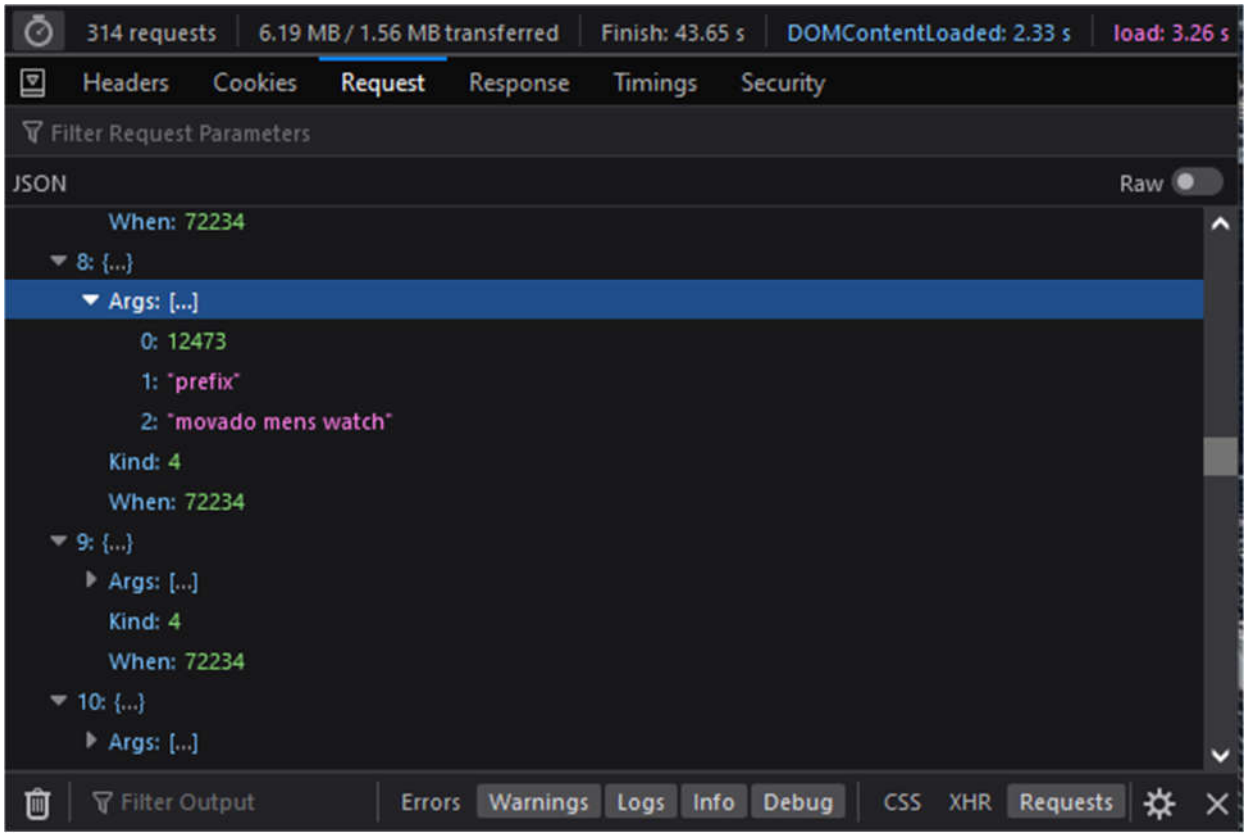
49. Plaintiff has visited www.bloomingdales.com while in Missouri. Specifically, Plaintiff visited www.bloomingdales.com via the web browser on both her mobile phone and computer.

50. While visiting Bloomingdale's website, Plaintiff fell victim to Defendant's unlawful monitoring, recording, and collection of Plaintiff's Website Communications with www.bloomingdales.com.

51. Unknown to Plaintiff, Bloomingdale's procures and embeds session replay technology on its website.

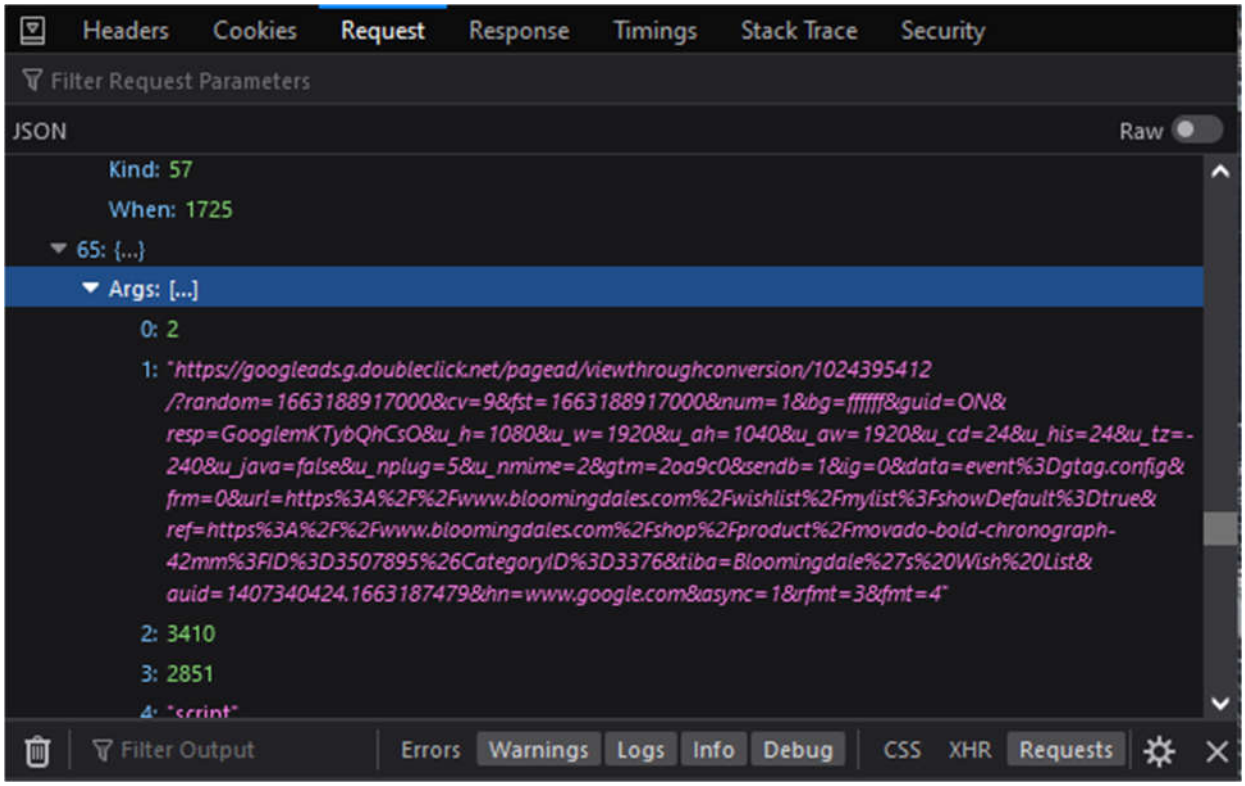
52. During the website visit, Plaintiff's Website Communications were captured by session replay technology and sent to various third party vendors.

53. For example, when visiting www.bloomingdales.com, if a website user views a product, that information is captured by the session replay technology embedded on the website:



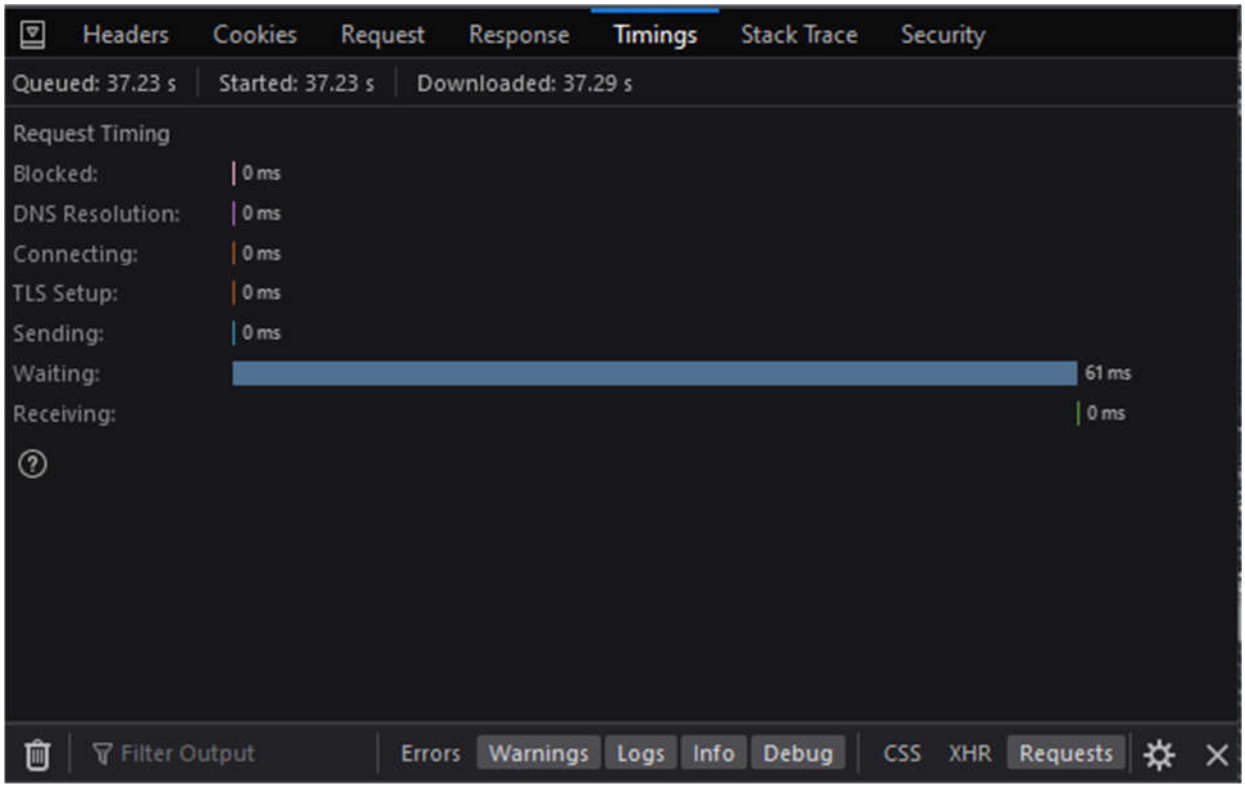
Depicting information sent to one of the third party vendors—FullStory—through a session replay technology—FullStory Script—after searching for "movado mens watch" while visiting www.bloomingdales.com.

54. Similarly, when a user adds a product onto their "Wish List" on www.bloomingdales.com, that information is sent to third party vendors:



Depicting information sent to one of the third party vendors—FullStory—through a session replay technology—FullStory Script—after adding a "Movado BOLD Chronograph, 42 mm" to a wish list on www.bloomingdales.com.

55. The eavesdropping by the session replay technology is ongoing during the visit and intercepts the contents of these communications between Plaintiff and Bloomingdale's with instantaneous transmissions to the third party vendors, as illustrated below, in which only 61 milliseconds were required to send a packet of even response data, which would indicate whatever the website user had just done:



56. The session replay technology operates in the same manner for all putative Class members.

57. Like Plaintiff, each Class member visited www.bloomingdales.com with session replay technology embedded in it, and that session replay technology intercepted the Class members' Website Communications with www.bloomingdales.com by sending hyper-frequent logs of those communications to third party vendors.

58. Even if Bloomingdale's masks certain elements when it configures the settings of the session replay technology embedded on its website, any operational iteration of the session replay technology will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

59. For example, even with heightened masking enabled, third party vendors will still learn through the intercepted data exactly which pages a user navigates to, how the user moves

through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

60. As a specific example, if a user types a product into Bloomingdale's main search bar and initiates a search, even if the text entered into the search bar is masked, third party vendors will still learn what is entered into the bar as soon as the search result page loads. This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by Bloomingdale's will repeat the searched information back on the generated page. That information will not be masked even if user-inputted text is fully masked in a text field.

61. Plaintiff reasonably expected that her visits to Defendant's website would be private and that Defendant would not be watching, tracking, and recording Plaintiff as she browsed and interacted with the website, particularly because Plaintiff was never presented with any type of pop-up disclosure or consent form alerting Plaintiff that her visits to the website were being watched and recorded by Defendant. Moreover, she used her own personal device to communicate with the website, was not aware of anyone else present during the communication and presumed her private interactions with Defendant's website were just that: private.

62. Plaintiff reasonably believed that she was interacting privately with Defendant's website, and not that she was being watched and recorded and that those recordings could later be watched again and again by Defendant's employees, or worse yet, live while Plaintiff was on the website.

63. The third-party vendor that provided the session replay technology to Defendant is not a provider of wire or electronic communication services, or an internet service provider.

64. Defendant is not a provider of wire or Electronic Communication services, or an internet service provider.

65. Defendant utilized session replay technology to intentionally and contemporaneously watch and intercept the substance and content of Plaintiff's Electronic Communications with Defendant's website, including mouse clicks and movements, keystrokes, substantive information inputted by Plaintiff, pages and content viewed by Plaintiff, and scroll movements, and copy and paste actions. In other words, Defendant intercepted, stored, and recorded the webpages visited by Plaintiff, as well as everything Plaintiff did on those pages, what Plaintiff looked at, and the information Plaintiff inputted.

66. The third party vendor intentionally utilized by Defendant contemporaneously watched and intercepted the content of electronic computer-to-computer data communications between Plaintiff's computer and/or mobile device and the computer servers and hardware utilized by Defendant to operate its website—as the communications were transmitted from Plaintiff's computer and/or mobile device to Defendant's computer servers and hardware—and while viewing, copied and sent and/or re-routed the communications to a storage file within the third party vendor's server. The intercepted data was transmitted contemporaneously to the third party vendor's server as it was sent from Plaintiff's computer and/or mobile device.

67. The session replay technology utilized by Defendant acts as an electronic, mechanical or other analogous device or apparatus in that the session replay technology monitors, intercepts and records the content of electronic computer-to-computer communications between Plaintiff's computer and/or mobile device and the computer servers and hardware utilized by Defendant to operate its website.

68. The session replay technology utilized by Defendant is not a website cookie, standard analytics tool, tag, web beacon, or other similar technology.

69. The data collected by Defendant identified specific information inputted and

content viewed, and thus revealed personalized and sensitive information about Plaintiff's Internet activity and habits.

70. The Electronic Communications intentionally watched and intercepted by Defendant was content generated through Plaintiff's intended use, interaction, and communication with Defendant's website relating to the substance and/or meaning of Plaintiff's communications with the website (*i.e.*, mouse clicks and movements, keystrokes, information inputted by Plaintiff, and pages and content clicked on and viewed by Plaintiff). This information is "content" as defined by the Missouri Wiretapping Act and is not merely record information regarding the characteristics of the message that is generated in the course of the communication, nor is it simply information disclosed in the referrer headers. The mere fact that Defendant values this content, monitors, intercepts and records it, confirms these communications are content that convey substance and meaning to Defendant.

71. The Electronic Communications intentionally intercepted by Defendant were not generated automatically and were not incidental to Plaintiff's communications.

72. The session replay technology utilized by Defendant watched, intercepted, copied, replicated, and sent the data in a manner that was undetectable by Plaintiff.

73. The session replay technology utilized by Defendant gave Defendant the ability to view Plaintiff's website visits live in real-time as they were occurring and intercept the content of these Electronic Communications as they were occurring, which is exactly what Defendant did.

74. These electronic data communications were not only watched in real-time, intercepted contemporaneously with transmission and stored, but could also be used by Defendant to create a video playback of Plaintiff's visit to the website. Defendant's contemporaneous interception of Plaintiff's Electronic Communications during transmission allowed Defendant to

observe, capture, and divulge Plaintiff's personal interests and habits as she interacted with and browsed Defendant's website in real-time.

75. Defendant similarly intercepted Electronic Communications of at least thousands of other individuals located in Missouri who visited Defendant's website.

76. Defendant did not utilize a telephone or telegraph instrument, equipment, or facility to intercept Plaintiff's and the Class Members' Electronic Communications at issue. Rather, Defendant utilized a spyware embedded within its website to watch and intercept the communications at issue. By the very nature of its operation, said spyware is the equivalent of a device or apparatus used to intercept wire or Electronic Communications.

77. Defendant never alerted or asked Plaintiff or the Class Members for permission to watch, intercept and record their visits to Defendant's website using session replay technology.

78. Plaintiff and the Class Members never consented to being watched or having their Electronic Communications on Defendant's website intercepted by Defendant or anyone acting on Defendant's behalf, and they were never given the option to opt out of Defendant's surreptitious watching and recording.

79. Plaintiff and the Class Members never provided Defendant, its employees, or agents with consent to watch and intercept and record their Electronic Communications using session replay technology.

80. Plaintiff and the Class Members did not specifically, clearly, and unmistakably consent to Defendant's watching, interception and recording of their Electronic Communications using session replay technology.

81. Plaintiff and the Class Members did not have a reasonable opportunity to discover Defendant's unlawful interceptions because Defendant did not disclose that it was watching their

activity, nor did Defendant disclose its interception, nor did it seek consent from Plaintiff and the Class Members prior to interception of their communications.

82. Plaintiff and the Class Members never clicked or otherwise agreed to any disclosure or consent form authorizing Defendant to watch and intercept Plaintiff's and the Class Members' Electronic Communications using session replay technology.

83. Defendant intercepted Plaintiff's and the Class Members' Electronic Communications from the moment they landed on Defendant's website, and before they had an opportunity to even consider consenting or agreeing to any privacy or terms of use policy on the website. Defendant's unlawful watching and interception occurred before Plaintiff and the Class Members were given an opportunity to review, let alone consent, to any language that Defendant may claim purportedly authorized its violations of the Missouri Wiretapping Act or other acts or laws.

84. Defendant's website failed to explicitly alert or otherwise notify Plaintiff and the Class Members that Defendant would be utilizing session replay technology to monitor and record their interactions with Defendant's website.

85. Upon immediately landing on Defendant's website, Plaintiff and the Class Members were not alerted that by entering the website Defendant would unilaterally attempt to bind them to Defendant's terms and policies or privacy policy. Indeed, the landing page to Defendant's website not only fails to advise visitors that Defendant is intercepting their Electronic Communications, but it also does not contain any type of conspicuous disclosure regarding Defendant's terms of use or privacy policy.

86. Plaintiff and the Class Members were not immediately required to click on any box or hyperlink containing Defendant's terms of use or privacy policy upon visiting the website or in

order to navigate through the website.

87. Plaintiff and the Class Members were not placed on notice of Defendant's terms and policies or privacy policy upon immediately visiting the website. Instead, Defendant's terms of use and privacy policy are buried at the bottom of Defendant's website where Plaintiff and the Class Members were unable to see them.

88. Defendant does not require visitors to its website to immediately and directly acknowledge that the visitor has read Defendant's terms of use or privacy policy before proceeding to the site. In other words, Defendant's website does not immediately direct visitors to the site to the terms of use or privacy policy and does not require visitors to click on a box to acknowledge that they have reviewed the terms and conditions/policy in order to proceed to the website.

89. There is no cookie banner that Plaintiff and Class Members must affirmatively ex out of for it to no longer be visible on the Defendant's website.

90. Defendant's entire website, including its terms of use and privacy policy, are silent on Defendant's use of session replay technology to watch, monitor and record Plaintiff's and the Class Members' (1) mouse clicks and movements; (2) keystrokes; (3) substantive information inputted into the website; and (4) pages and content viewed.

91. Defendant's use of session replay technology was not instrumental or necessary to the operation or function of Defendant's website or business.

92. Defendant's use of a Session Replay Provider to contemporaneously intercept Plaintiff's Electronic Communications at the time of transmission was not instrumental or necessary to Defendant's provision of any of its goods or services. Rather, the level and detail of information surreptitiously collected by Defendant indicates that the only purpose was to gain an unlawful understanding of the habits and preferences of users to its website, and the information

collected was solely for Defendant's own benefit.

93. At least one of the purposes for Defendant to watch and intercept Plaintiff's and the Class Members' Electronic Communications was to allow Defendant to learn of Plaintiff's and the Class Members' personal preferences, which would then be used to market Defendant's services and goods to Plaintiff and the Class Members.

94. Plaintiff and the Class Members had a reasonable expectation of privacy during their visits to Defendant's website, which Defendant violated by intentionally monitoring and intercepting the content of their Electronic Communications with the website.

95. The purpose of the Missouri Wiretapping Act is to protect every person's right to privacy and to prevent the pernicious effect on browsers who would otherwise feel insecure from intrusion into their browsing activity.

96. Defendant's covert monitoring and interception of Plaintiff's and the Class Members' Electronic Communications caused Plaintiff and the Class Members harm, including violations of their substantive legal privacy rights under the ECPA, FSCA, and CFAA, invasion of privacy, invasion of their rights to control information concerning their person, and/or the exposure of their private information. Moreover, Defendant's practices caused harm and a material risk of harm to Plaintiff's and the Class Members' privacy and interest in controlling their personal information, habits, and preferences.

97. Additionally, Defendant's actions constitute a trespass to Plaintiff's and the Class's chattels and/or a conversion of Plaintiff's and the Class's chattels.

CLASS ACTION ALLEGATIONS

98. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

> All natural persons in the United States (1) who visited Defendant's website, www.bloomingdales.com, and (2) whose electronic communications were intercepted by Defendant or on Defendant's behalf (the "Nationwide Class").

99. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following sub-Class:

> All natural persons in the State of Missouri (1) who visited Defendant's website, www.bloomingdales.com, and (2) whose electronic communications were intercepted by Defendant or on Defendant's behalf (the "Missouri Class").

100. The Nationwide Class and the Missouri Class are collectively referred to herein as the "Class" and members of the Nationwide Class and Missouri Class are collectively referred to as "Class Members."

101. Excluded from the Class are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

102. **Numerosity:** The members of the Class are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of Bloomingdale's or the Session Replay Providers.

103. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: (a) whether Defendant employed Session Replay Providers to intercept and record Bloomingdale's website visitors' Website Communications; (b) whether Defendant operated or participated in the operation of an eavesdropping device; (c) whether Defendant derives a benefit or information from the illegal use of an eavesdropping device; (d) whether Defendant directed another to use an eavesdropping device illegally on its behalf; (e) whether session replay technology is an "eavesdropping device"

used to intercept or record private electronic communications; (f) whether Defendant acquired the contents of website users' private electronic communications without their consent; (g) whether Plaintiff and Class members had a reasonable expectation of privacy in their Website Communications; (f) whether Defendant violated the Missouri Wiretap Act, Mo. Ann. Stat. §§ 542.400 *et seq*.; (g) whether Defendant's interception of Plaintiff's and Class members' private electronic communications is an unfair or deceptive act or practice; (h) whether Defendant's conduct violates the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010 *et seq.* (i) whether Defendant violated 18 U.S.C. § 2510 and/or 2511, *et seq.*; (j) whether Defendant's conduct constitutes an Invasion of Privacy – Intrusion Upon Seclusion; (k) whether Defendant's conduct constitutes a trespass to chattels; (l) whether Defendant's conduct constitutes a conversion to chattels; (m) whether Defendant violated 18 U.S.C. § 2701 and/or 2702, *et seq*. (the Electronic Stored Communications Act or "ESCA"); (n) whether Defendant violated 18 U.S.C. § 1030, *et seq*. (the Compute Fraud and Abuse Act); (o) whether Plaintiff and Class Members are entitled to equitable relief; and/or (p) whether Plaintiff and Class Members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

104. **Typicality:** Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each member of the Class had their electronic communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the members of the Class typical of one another.

105. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent

and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members of the Class.

106. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

107. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant intercepted Plaintiff's and Class members' Website Communications, then Plaintiff and each Class member suffered damages by that conduct.

108. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through Bloomingdale's books and records or the Session Replay Providers' books and records.

TOLLING

109. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that Plaintiff's information was intercepted because Defendant kept this information secret.

COUNT I
Violation of Missouri Wiretap Act,
Mo. Ann. Stat. §§ 542.400 *et seq.*
(On Behalf of Plaintiff and the Missouri Class)

110. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

111. Plaintiff brings this claim individually and on behalf of the Class.

112. The Missouri wiretap statute broadly prohibits the interception, disclosure or use of any wire, oral or electronic communication. Mo. Stat. § 542.402.

113. Any person whose wire communication is intercepted, disclosed, or used in violation of sections 542.400 to 542.422 shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications; and (2) be entitled to recover from any such person: (a) actual damages, but not less than liquidated damages computed at the rate of one hundred dollars a day for each day of violation or ten thousand dollars whichever is greater; (b) punitive damages on a showing of a willful or intentional violation of sections 542.400 to 542.422; and (c) A reasonable attorney's fee and other litigation costs reasonably incurred. Mo. Stat. § 542.418.

114. "Wire communication" is defined as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception including the use of such connection in a switching station furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of local, state or interstate

communications." Mo. Stat. § 542.400(12).

115. A "Person" is "defined as any employee, or agent of this state or political subdivision of this state, and any individual, partnership, association, joint stock company, trust, or corporation." Mo. Stat. § 542.400(9).

116. "Intercept" is defined as "the aural acquisition of the contents of any wire communication through the use of any electronic or mechanical device, including but not limited to interception by one spouse of another spouse." Mo. Stat. § 542.400(6).

117. "Electronic, mechanical, or other device" is defined as "any device or apparatus which can be used to intercept a wire communication other than: (a) Any telephone or telegraph instrument, equipment or facility, or any component thereof, owned by the user or furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or being used by a communications common carrier in the ordinary course of its business or by an investigative office or law enforcement officer in the ordinary course of his duties; or (b) A hearing aid or similar device being used to correct subnormal hearing to not better than normal." Mo. Stat. § 542.400(5).

118. "Contents," "when used with respect to any wire communication, includes any information concerning the identity of the parties, the substance, purport, or meaning of that communication." Mo. Stat. § 542.400(3).

119. An "Aggrieved person" is defined as "a person who was a party to any intercepted wire communication or a person against whom the interception was directed." Mo. Stat. § 542.400 (1).

120. Bloomingdale's is a "Person" for purposes of the Act because it is a corporation.

121. Session replay technology like that utilized by Defendant, is an "electronic,

mechanical or other device" used to transcribe electronic communications and to intercept a wire communication within the meaning of the Act.

122. The third party vendors are not a party to the Website Communications—Plaintiff and the Class only knew they were communicating with Bloomingdale's, not the Session Replay Providers.

123. Plaintiff's and Class members' intercepted Website Communications constitute wire communications within the meaning of the Act.

124. Bloomingdale's intentionally operated and employed session replay technology on its website to spy on, automatically and secretly, and intercept its website visitors' private electronic interactions and communications with Bloomingdale's in real time, which are Contents within the meaning of the Act.

125. Plaintiff's and Class members' private electronic communications were intercepted contemporaneously with their transmission.

126. Plaintiff and Class members had a reasonable expectation of privacy in their Website Communications based on the detailed information the session replay technology collected from Plaintiff and Class members.

127. Plaintiff and Class members did not consent to having their Website Communications surreptitiously intercepted and recorded and are Aggrieved persons within the meaning of the Act.

128. The Missouri Wiretap Act exception to exception applies. Under Mo. Stat. § 542.402.2(3), it is permissible "[f]or a person not acting under law to intercept a wire communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception **unless such communication is**

intercepted for the purpose of committing any criminal or tortious act." (Emphasis added.) Plaintiff's communication was intercepted for the purpose of invading the privacy of Plaintiff and the Missouri Class and is thus subject to this exception.

129. Pursuant to Mo. Stat. § 542.418, Plaintiff and Class members are entitled to: (1) actual damages; (2) statutory damages including liquidated damages at $100 per day of violation or $10,000, whichever is greater, and (3) punitive damages. Plaintiff is also entitled to an award of attorney's fees and expenses.

130. Bloomingdale's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with session replay technology enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II
Violation of Missouri's Merchandising Practices Act
Mo. Rev. Stat. § 407.010 *et seq.*
(On Behalf of Plaintiff and the Missouri Class)

131. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

132. Plaintiff brings this claim individually and on behalf of the Class.

133. The Missouri Merchandising Practice Act (for the purposes of this section, "MPA") protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

134. The Missouri MPA makes unlawful the "act, use or employment by any person of any deception, fraud, false pretense, misrepresentation, unfair practice, or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce." Mo. Rev. Stat. § 407.020.

135. Plaintiff, individually and on behalf of the Class, is entitled to bring this action

pursuant to Mo. Rev. Stat. § 407.025, which provides in relevant part that: (a) Any person who purchases or leases merchandise primarily for personal, family or household purposes and thereby suffers an ascertainable loss of money or property, real or personal, as a result of the use or employment by another person of a method, act or practice declared unlawful by section 407.020, may bring a private civil action in either the circuit court of the county in which the seller or lessor resides or in which the transaction complained of took place, to recover actual damages. The court may, in its discretion, award to the prevailing party attorney's fees, based on the amount of time reasonably expended, and may provide such equitable relief as it deems necessary or proper.

136. Bloomingdale's is a "person" within the meaning of the Mo. Rev. Stat. § 407.010(5) in that Bloomingdale's is a domestic "[…] for-profit […] corporation."

137. Plaintiff and members of the Class are "persons" under the MMPA in that they are natural persons, and they visited www.bloomingdales.com to utilize the Bloomingdale's search engine for personal, family, and/or household use. Furthermore, Plaintiff Ann Jones visited www.bloomingdales.com to utilize the Bloomingdale's search engine to shop for, purchase, and/or contract to purchase "merchandise" for personal, family, and/or household use.

138. The MPA applies to Bloomingdale's conduct described herein because it protects consumers in transactions that are intended to result, or which have resulted in the sale of goods or services.

139. The MMPA defines "merchandise" as any objects, wares, goods, commodities, intangibles, real estate, or services. *See* Mo. Rev. Stat. § 407.010. Thus, the items for sale on www.bloomingdales.com are merchandise within the meaning of the Act. Additionally, the website and the search engine thereon is a service which is used by Bloomingdale's in connection with the sale or advertisement of any merchandise in trade or commerce.

140. "Trade" or "commerce" is defined as "the advertising, offering for sale, sale, or distribution, or any combination thereof, of any services and any property, tangible or intangible, real, personal, or mixed, and any other article, commodity, or thing of value wherever situated." Bloomingdale's advertising, offering for sale, and sale of its real estate search engine and the real estate located thereon on www.bloomingdales.com is considered "trade" or "commerce" in the State of Missouri within the meaning of Mo. Rev. Stat. § 407.010(7).

141. The Missouri Attorney General has promulgated regulations defining the meaning of unfair practice as used in the above statute. Specifically, Mo. Code Regs. tit. 15, § 60-8.020, provides:

(1) An unfair practice is any practice which—

(A) Either—

1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or

2. Is unethical, oppressive or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

(2) Proof of deception, fraud, or misrepresentation is not required to prove unfair practices as used in section 407.020.1., RSMo. (*See, Federal Trade Commission v. Sperry and Hutchinson Co.*, 405 U.S. 233, 92 S.Ct. 898, 31 L.Ed.2d 170 (1972); *Marshall v. Miller*, 302 N.C. 539, 276 S.E.2d 397 (N.C. 1981); *see also*, Restatement, Second, Contracts, sections 364 and 365).

142. Pursuant to Mo. Rev. Stat. §407.020 and Mo. Code Regs. Tit. 15, § 60- 8.020, Defendant's acts and omissions fall within the meaning of "unfair."

143. Missouri case law provides that the MMPA's "literal words cover *every practice imaginable and every unfairness to whatever degree*." *Conway v. CitiMortgage, Inc.*, 438 S.W.3d 410, 416 (Mo. 2014) (quoting *Ports Petroleum Co., Inc. of Ohio v. Nixon*, 37 S.W.3d237, 240 (Mo. banc 2001). Furthermore, the statute's "plain and ordinary meaning of the words themselves . . . are unrestricted, all-encompassing and exceedingly broad." *Id.* at 240.

144. Bloomingdale's violated the MMPA by omitting and/or concealing material facts about www.bloomingdales.com. Specifically, Bloomingdale's omitted and/or concealed that it directed third party vendors to secretly monitor, collect, transmit, and discloses its website visitors' Website Communications to the third party vendors using session replay technology.

145. Bloomingdale's direction and employment of the Session third party vendors and their session replay technology to intercept, collect, and disclose website visitors' Website Communications are material to the transactions on www.bloomingdales.com. Bloomingdale's does not disclose its use of session replay technology to secretly monitor and collect website visitors' Website Communications. Had Plaintiff and Class members known that the session replay spyware (that collects, transmits, and discloses Website Communications to the Session Replay Providers) were embedded in Bloomingdale's website, they would not have visited www.bloomingdales.com to shop for, purchase, or contract to purchase merchandise or they would have required Bloomingdale's to compensate them for the interception, collection, and disclosure of their Website Communications.

146. Bloomingdale's intentionally concealed interception, collection, and disclosure of website visitors' Website Communications using session replay technology embedded in www.bloomingdales.com is material because it knows that consumers would not otherwise visit its website to search for, purchase, and contract to purchase merchandise. Indeed, Bloomingdale's

concealment of such facts was intended to mislead consumers.

147. Bloomingdale's concealment, suppression, and/or omission of material facts was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the MMPA.

148. By failing to disclose and inform Plaintiff and the Class about its interception, collection, and disclosure of website visitors' Website Communications, Bloomingdale's engaged in acts and practices that constitute unlawful practices in violation of Mo. Ann. Stat. §§ 407.010, *et seq.*

149. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and each member of the Class has suffered actual harm in the form of money and/or property because the disclosure of their Website Communications has value as demonstrated by the collection and use of it by Bloomingdale's. The collection and use of this information has now diminished the value of such information to Plaintiff and the Class.

150. As such, Plaintiff and the Class seek an order (1) requiring Bloomingdale's to cease the unfair practices described herein; (2) awarding actual damages; and (3) awarding reasonable attorneys' fees and costs. Plaintiff and the Class seek all relief available under Mo. Ann. Stat. § 407.020, which prohibits "the act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce…," as further interpreted by Mo. Code Regs. Ann. tit. 15, §§ 60-7.010, *et seq.*, Mo. Code Regs. Ann. tit. 15, §§ 60-8.010, *et seq.*, and Mo. Code Regs. Ann. tit. 15, §§ 60-9.010, *et seq.*, and Mo. Ann. Stat. § 407.025, which provides for the relief sought in this count.

151. Bloomingdale's conduct is ongoing, and it continues to unlawfully intercept the

communications of Plaintiff and Class members any time they visit Defendant's website with session replay technology enabled without their consent. Plaintiff and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT III
Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Missouri Class)

152. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

153. Under Missouri law, the general tort of invasion of privacy describes four distinct torts under Missouri law: (1) unreasonable intrusion upon the seclusion of another; or (2) appropriation of the other's name or likeness; or (3) unreasonable publicity given to the other's private life; or (4) publicity that unreasonably places the other in a false light before the public. Plaintiff states a claim for unreasonable intrusion upon the seclusion of another.

154. Plaintiff brings this claim individually and on behalf of the Class.

155. Plaintiff and Class members have an objective, reasonable expectation of privacy in their Website Communications.

156. Plaintiff and Class members did not consent to, authorize, or know about Bloomingdale's intrusion at the time it occurred. Plaintiff and Class members never agreed that Bloomingdale's could collect or disclose their Website Communications.

157. Plaintiff and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

158. Bloomingdale's intentionally intruded on Plaintiff's and Class members' private life, seclusion, or solitude, without consent.

159. Bloomingdale's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

160. Plaintiff and Class members were harmed by Bloomingdale's wrongful conduct as Bloomingdale's conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their Website Communications.

161. Bloomingdale's conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

162. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff's and Class members' property.

163. Further, Bloomingdale's has improperly profited from its invasion of Plaintiff and Class members' privacy in its use of their data for its economic value.

164. As a direct and proximate result of Bloomingdale's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

165. Bloomingdale's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with session replay technology enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT IV
Trespass to Chattels

(On Behalf of Plaintiff and the Missouri Class)

166. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

167. Plaintiff and the Missouri Class owned, possessed, and/or had a right to possess Plaintiff's computer and/or the data in contained therein.

168. Plaintiff and the Missouri Class owned, possessed, and/or had a right to possess Plaintiff's mobile device and/or the data in contained therein.

169. As set forth above, Defendant intentionally interfered with: (a) Plaintiff's and the Missouri Class's use and/or possession of Plaintiff's computer and/or mobile device; and/or (b) Plaintiff's and the Missouri Class's use and/or possession of the data contained on Plaintiff's computer and/or mobile device as described above.

170. Plaintiff and the Missouri Class did not consent to the aforementioned interference.

171. The aforementioned interference was the actual and proximate cause of injury to Plaintiff and the Missouri Class members because it exposed their respective private and/or personally identifiable information and/or data to one or more third parties.

172. Additionally, the interference gave third parties the data and information without the consent of Plaintiff and the Missouri Class and which is valuable and for which Defendant did not obtain informed consent nor pay Plaintiff or the Missouri Class to obtain.

173. Plaintiff and the Missouri Class members are entitled to recover the actual damages they suffered as a result of Defendant's aforementioned interference with their respective computer and/or mobile devices in an amount to be determined at trial.

COUNT V
CONVERSION TO CHATTELS
(On Behalf of Plaintiff and the Missouri Class)

174. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

175. Plaintiff and the Missouri Class owned, possessed, and/or had a right to possess their respective computer and/or mobile device and/or the data contained therein.

176. As set forth above, Defendant intentionally interfered with: (a) Plaintiff's and the Missouri Class's use and/or possession of their respective computer and/or mobile device; and/or (b) Plaintiff's and the Missouri Class's use and/or possession of the data contained on their respective their respective computer and/or mobile device as described above.

177. Defendant obtained or exercised unauthorized control over the personal property of Plaintiff and the Missouri Class, without the consent of Plaintiff and the Missouri Class.

178. Plaintiff and the Missouri Class Members were deprived of their respective right to possession.

179. Defendant exercised dominion and ownership over Plaintiff's and the Missouri Class's personalty inconsistent with, and in denial of, the rights of Plaintiff's and the Missouri Class.

180. Plaintiff and the Missouri Class did not consent to the aforementioned interference.

181. The aforementioned interference was the actual and proximate cause of injury to Plaintiff and the Missouri Class Members because it exposed their respective private and/or personally identifiable information and/or data to one or more third parties.

182. Additionally, the interference gave third parties the data and information without the consent of Plaintiff and the Missouri Class, and which is valuable, and for which Defendant did not obtain informed consent nor pay Plaintiff or the Missouri Class to obtain.

183. Plaintiff and the Missouri Class Members are entitled to recover the actual damages

they suffered as a result of Defendant's aforementioned interference with their respective computer and/or mobile device in an amount to be determined at trial.

COUNT VI
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA)
18 U.S.C. § 2511(1) *et seq*.
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On Behalf of the Plaintiff and the Nationwide Class and the Missouri Class)

184. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

185. The ECPA protects both sending and receipt of communications.

186. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

187. The transmissions of Plaintiff's Electronic Communications qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

188. **Electronic Communications**. The transmission of data between Plaintiff and Class Members and Defendant's websites with which they chose to exchange communications are "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo optical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

189. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include [] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

190. **Interception.** The ECPA defines the interception as the "acquisition of the contents

of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents . . . include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

191. **Electronic, Mechanical, or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device . . .which can be used to intercept a[n] . . . electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Defendant's web-servers;

d. Defendant's web-servers where the session replay technology was implemented; and

e. The session replay technology deployed by Defendant to effectuate the sending and acquisition of patient communications

192. By utilizing and embedding session replay technology on the webpages of www.bloomingdales.com, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the Electronic Communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

193. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the Third party vendors by inserting the computer software into the web browser and capturing virtually every action conducted by Plaintiff and Class Members on Defendant's website.

194. Defendant's intercepted communications include, but are not limited to, all mouse

movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through the website.

195. By intentionally disclosing or endeavoring to disclose the electronic communications of the Plaintiff and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

196. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

197. **Unauthorized Purpose**. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' Electronic Communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

198. Defendant intentionally used the wire or Electronic Communications to increase its profit margins.

199. Defendant's interception of the contents of Plaintiff's and Class Members' communications was contemporaneous with their exchange with the websites to which they directed their communications. As described above, the session replay technology process occurs in milliseconds while the communication is still being exchanged between Plaintiff and Class Members and the website to which they directed their communications. The signal issued by session replay technology is sent simultaneously with the signal sent to websites to which

Plaintiff's and Class Members' communications were directed.

200. Defendant was not acting under color of law to intercept Plaintiff's and the Class Members' wire or electronic communications.

201. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy.

202. Plaintiff and Class Members did not give prior consent to Defendant intercepting their wire and/or Electronic Communications on Defendant's website for purposes of invading Plaintiff's privacy via the third party vendors.

203. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

204. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions, including as described above the following: (1) a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person; and (2) violation of state unfair business statutes.

COUNT VII
VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE 18 U.S. Code § 2511(3)(a)
(On Behalf of Plaintiff and the Nationwide Class and the Missouri Class)

205. Plaintiff incorporates all preceding paragraphs as though set forth herein.

206. The ECPA Wiretap statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such

communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

207. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

208. Defendant's web browser is an Electronic Communication service. It provides to users thereof the ability to send or receive Electronic Communications. In the absence of a web browser or some other system, internet users could not send or receive communications over the internet regarding that which the Plaintiff or Class Members are looking for and that which the entity is selling.

209. **Intentional Divulgence**. Defendant intentionally designed the web browser so that it would divulge the contents of Plaintiff's and Class Members' communications via the session replay technology.

210. **While in Transmission**. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications was contemporaneous with their exchange with the websites, to which they directed their communications. As described above, the session replay technology process occurs in milliseconds while the communication is still being exchanged between Plaintiff and Class Members and the websites to which they directed their communications.

211. Defendant divulged the contents of Plaintiff's and Class Members' electronic communications without authorization. Defendant divulged the contents of Plaintiff's and Class Members' communications to Third party vendors without Plaintiff's and Class Members' consent and/or authorization.

212. **Exceptions do not apply**. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act states that "[a] person or entity providing

electronic communication service to the public may divulge the contents of any such communication":

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"
b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;"
c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or
d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

U.S.C. § 2511(3)(b).

213. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

214. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on Defendant's website to session replay technology was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of the www.bloomingdales.com service; nor (2) necessary to the protection of the rights or property of Defendant.

215. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

216. Defendant's divulgence of the contents of user communications on Defendant's browser through session replay technology was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and

(b) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiff and Class Members were exchanging information.

217. Moreover, Defendant divulged the contents of Plaintiff and Class Members' communications through the session replay technology to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

218. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

219. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT VIII
VIOLATION OF
TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2701 *et seq*.
(On Behalf of Plaintiff and the Nationwide Class and the Missouri Class)

220. Plaintiff incorporates all preceding paragraphs as though set forth herein.

221. The Stored Communications Act (hereinafter "SCA") provides a cause of action against any person who "intentionally accesses without authorization a facility through which an electronic communication service is provided," or any person "who intentionally exceeds an authorization to access that facility; and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. § 2701(a).

222. The SCA defines "electronic storage" as "any temporary, intermediate storage of a

wire or electronic communication incidental to the electronic transmission thereof;" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

223. The SCA defines an "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

224. Defendant intentionally accessed without authorization or intentionally exceeded authorization to access facilities through which an electronic communications services was provided when they used the instrumentalities described in this Complaint to access the Plaintiff's web-browsers and computing devices for purposes of tracking the Plaintiff's electronic communications as defined above.

225. The devices utilized by the Plaintiff and/or the web browsers on said devices provide electronic communications services to the Plaintiff because they "provide to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

226. Plaintiff did not authorize or provide consent to the extent of the Defendant's access to Plaintiff and the Class's computing devices.

227. Plaintiff's devices store information typed into the website, among other things.

228. The Plaintiff's respective web browsers store information in browser-managed files on the Plaintiff's computing devices. These browsers are also facilities under the SCA because they comprise the spyware necessary for and "through which (the) electronic communications service is provided."

229. Defendant intentionally accessed Plaintiff's web browsers without authorization when it embedded and used third party vendors to access Plaintiff's browser and device

immediately upon the Plaintiff's visiting Defendant's websites and after sign-up without obtaining the consent of the Plaintiff.

230. Plaintiff's computing devices are facilities under the SCA because they comprise the hardware necessary for and "through which (the) electronic communications service is provided."

231. By embedding and utilizing session replay technology, Defendant "intentionally accesse[d] without authorization a facility through which an electronic communication service is provided," or "intentionally exceed[ed] an authorization to access that facility", Defendant thereby obtained "access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. § 2701(a).

232. Through the session replay technology embedded by Defendant, website users' website activities and communications are accessed within milliseconds of their occurrence. For that reason, when Defendant accesses these facilities to acquire Plaintiff's electronic communications, it acquires profile information and related just-transmitted electronic communications. Defendant acquires the profile information and related electronic communications out of electronic storage, incidental to the transmission thereof.

233. Plaintiff and Class Members were harmed by Defendant's violations, and pursuant to 18 U.S.C. § 2707(c), are entitled to actual damages including profits earned by Defendant attributable to the violations or statutory minimum damages of $1,000 per person, punitive damages, costs, and reasonable attorney's fees.

COUNT IX
VIOLATION OF TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2702, *et seq*.
(On Behalf of Plaintiff and the Nationwide Class and the Missouri Class)

234. Plaintiff incorporates all preceding paragraphs as though set forth herein.

235. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

236. **Electronic Communication Service.** ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

237. Defendant intentionally procures and embeds various session replay technology from a third party vendor on its website to track and analyze website user interactions and communications with www.bloomingdales.com. Defendant's session replay technology from a third party vendor on its website qualifies as an Electronic Communication Service.

238. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

239. Defendant stores the content of Plaintiff's and Class Members' communications on Defendant's browser and files associated with it.

240. Specifically, Defendant stores the content of Plaintiff's and Class Members' communications within Defendant's browser in two ways: (a) for purposes of backup protection so that if the browser inadvertently shuts down, Plaintiff and Class Members can be presented with the option to restore their previous communications; and (b) for a temporary and intermediate amount of time incidental to the electronic transmission thereof when it places the contents of a user communications into the browser's web-browsing history, which is only kept on the browser

for 90 days.

241. When Plaintiff or Class Member makes an electronic communication, the content of that communication is immediately placed into storage.

242. Defendant knowingly divulges the contents of Plaintiff's and Class Members' communications through the session replay technology.

243. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication—"

a. to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."
b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;"
c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;"
d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;"
e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;"
f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A."
g. "to law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;"
h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or
i. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

244. Defendant did not divulge the contents of Plaintiff's and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiff and Class Members.

245. Sections 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

246. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

247. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on Defendant's website to third party vendors was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of the Chrome Service; nor (2) necessary to the protection of the rights or property of Defendant.

248. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

249. Defendant's divulgence of the contents of user communications on Defendant's browser through session replay technology was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiff and Class Members were exchanging information.

250. Moreover, Defendant divulged the contents of Plaintiff and Class Members' communications through the session replay technology to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

251. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their

communications to a law enforcement agency.

252. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT X
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (CFAA)
18 U.S.C. § 1030, *et seq*.
(On Behalf of Plaintiff and the Nationwide Class and the Missouri Class)

253. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully set forth herein.

254. The Plaintiff's and the Class's computer and/or mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

255. Defendant exceeded, and continues to exceed, authorized access to the Plaintiff's and the Class's protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

256. Defendant's conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiff's and the Class's private and personally identifiable data and content—including the website visitor's Electronic Communications with the website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communication which were never intended for public consumption.

257. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of Plaintiff and the Class being made available to Defendant, the third party vendor, and/or other third parties without adequate legal privacy protections.

258. Accordingly, Plaintiff and the Class are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Class, respectfully requests that the Court enter judgment in Plaintiff's and the Class's favor and against Defendant as follows:

A. Certifying the Class and appointing Plaintiff as the Class representative;

B. Appointing Plaintiff's counsel as class counsel;

C. Declaring that Defendant's past conduct was unlawful, as alleged herein;

D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;

E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, [30] and nominal damages, as well as restitution and/or disgorgement of

[30] Recent changes to the Missouri Merchandising Practices Act (MMPA) provide that:

> A claim for punitive damages shall not be contained in the initial pleading and may only be filed as a written motion with permission of the court no later than 120 days prior to the final pretrial conference or trial date. The written motion for punitive damages must be supported by evidence. The amount of punitive damages shall not be based on harm to nonparties. A

profits unlawfully obtained;

G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

Date: January 19, 2023

By: */s/ Tiffany Marko Yiatras*

Tiffany Marko Yiatras, MOED Bar No. 58197MO
CONSUMER PROTECTION LEGAL, LLC
308 Hutchinson Road
Ellisville, Missouri 63011-2029
Tele: 314-541-0317
Email: tiffany@consumerprotectionlegal.com

Bryan L. Bleichner (MN #0326689),
Admitted *pro hac vice*
Philip J. Krzeski (OH #0095713),
Admitted *pro hac vice*
CHESTNUT CAMBRONNE PA
100 Washington Avenue S, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com

> pleading seeking a punitive damage award may be filed only after the court determines that the trier of fact could reasonably conclude that the standards for a punitive damage award, as provided in the act, have been met. The responsive pleading shall be limited to a response of the newly amended punitive damages claim.

Thus, Plaintiffs expressly disclaim punitive damages in this initial pleading; however, expect to file as a written motion with permission of the Court no later than 120 days prior to the final pretrial conference or trial date seeking punitive damages.

Kate M. Baxter-Kauf (MN #0392037), to seek admission *pro hac vice*
Karen Hanson Riebel (MN #0219770), to seek admission *pro hac vice*
Maureen Kane Berg (MN #033344X), to seek admission *pro hac vice*
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com
mkberg@locklaw.com

ATTORNEYS FOR PLAINTIFF AND THE CLASS

CERTIFICATE OF SERVICE

I hereby certify that, on January 19, 2023, I electronically filed the foregoing with the Clerk of the Court by using the e-filing system which will send notification of such filing to all attorneys of record.

/s/ Tiffany Marko Yiatras